CLAIMS

We claim:

1. An apparatus, comprising:

an authentication device that authenticates a computing device, in communication with the authentication device, through employment of a determination that a current location of the authentication device matches an initial location of the authentication device.

2. The apparatus of claim 1, wherein the computing device comprises a first computing device

wherein the authentication device makes the determination that the current location of the authentication device matches the initial location of the authentication device in response to a request from a second computing device for authentication of the first computing device for a data transfer from the second computing device to the first computing device.

3. The apparatus of claim 2, wherein the request from the second computing device comprises an authentication challenge string;

wherein the authentication device stores one or more private keys, wherein if the current location of the authentication device matches the initial location of the authentication device, then the authentication device employs one or more of the one or more private keys to decrypt the authentication challenge string into an authentication challenge response.

4. The apparatus of claim 3, wherein the authentication device sends the authentication challenge response to the second computing device, wherein the second computing device analyzes the authentication challenge response to determine whether the first computing device is authenticated for the data transfer.

5. The apparatus of claim 4, wherein the second computing device comprises an authentication challenge key to compare with the authentication challenge response received from the authentication device;

wherein if the authentication challenge response matches the authentication challenge key, then the authentication challenge response represents that the first computing device is authenticated and the data transfer can be sent from the second computing device to the first computing device.

6. The apparatus of claim 3, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device prevents authentication of the first computing device and disables the one or more private keys.

7. The apparatus of claim 6, wherein the authentication device stores the one or more private keys in volatile memory, wherein upon determination that the current location of the authentication device does not match the initial location of the authentication device, the authentication device cuts off power to the volatile memory to erase the one or more private keys.

8. The apparatus of claim 1, wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the computing device;

wherein the base portion is fixed to a surface near the computing device, wherein the cover portion is fixed to the base portion to provide a secure shell for the one or more electronic components.

9. The apparatus of claim 8, wherein a first one of the base and cover portions receives electricity through a power port, wherein a second one of the base and cover portions receives electricity through an electrical contact with the first one of the base and cover portions;

wherein upon separation of the second one of the base and cover portions from the first one of the base and cover portions, the second one of the base and cover portions loses power and prevents authentication of the computing device.

10. The apparatus of claim 9, wherein the second one of the base and cover portions electrically supports one or more of the one or more electronic components that store one or more private keys, wherein the authentication device employs one or more of the one or more private keys to authenticate the computing device;

wherein a loss of power in the second one of the base and cover portions erases the one or more private keys from the one or more of the one or more electronic components.

11. The apparatus of claim 1, wherein the authentication device comprises a location sensor;

wherein upon initialization of the authentication device, the location sensor sets the initial location of the authentication device;

wherein the location sensor determines the current location of the authentication device, wherein the authentication device compares the current location with the initial location to authenticate the computing device.

12. The apparatus of claim 11, wherein the location sensor comprises a global positioning system component, wherein the global positioning system component measures the initial location and the current location of the authentication device as a three-dimensional location of latitude, longitude, and altitude.

13. The apparatus of claim 1, wherein the authentication device allows authentication of the computing device upon the determination that the current location of the authentication device matches the initial location of the authentication device within a specified error range.

14. A method, comprising the steps of:

receiving a request from a second computing device to authenticate a first computing device for a data transfer from the second computing device to the first computing device;

determining a current location of an authentication device, in communication with the first computing device, in response to the request from the second computing device; and

authenticating the first computing device if the current location of the authentication device matches an initial location of the authentication device.

15. The method of claim 14, wherein the request from the second computing device comprises an authentication challenge string, wherein the step of authenticating the first computing device if the current location of the authentication device matches the initial location of the authentication device comprises the steps of:

comparing the current location of the authentication device with the initial location of the authentication device; and

employing, if the current location of the authentication device matches the initial location of the authentication device, one or more private keys to decrypt the authentication challenge string into an authentication challenge response.

16. The method of claim 15, further comprising the steps of:

sending the authentication challenge response to the second computing device; and

analyzing the authentication challenge response to determine whether the first computing device is authenticated for the data transfer from the second computing device to the first computing device.

17. The method of claim 16, wherein the step of analyzing the authentication challenge response to determine whether the first computing device is authenticated for the data transfer from the second computing device to the first computing device comprises the steps of:

comparing the authentication challenge response with an authentication challenge key; and

determining that the data transfer can be sent from the second computing device to the first computing device if the authentication challenge response matches the authentication challenge key.

18. The method of claim 15, further comprising the steps of:

storing the one or more private keys in volatile or non-volatile memory; and

erasing the one or more private keys upon determination that the current location of the authentication device does not match the initial location of the authentication device.

19. The method of claim 15, further comprising the steps of:

storing the one or more private keys in volatile memory; and

discontinuing a power supply to the volatile memory to erase the one or more private keys upon determination that the current location of the authentication device does not match the initial location of the authentication device.

20. The method of claim 14, wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that store one or more private keys employable to authenticate the first computing device, the method further comprising the steps of:

attaching the base portion to a surface near the first computing device;

attaching the cover portion to the base portion to provide a secure shell for the one or more electronic components; and

erasing the one or more private keys if the cover portion is removed from the base portion.

21. The method of claim 14, wherein the authentication device comprises a base portion, a cover portion, and one or more electronic components that serve to authenticate the first computing device, the method further comprising the steps of:

attaching the base portion to a surface near the first computing device;

attaching the cover portion to the base portion to provide a secure shell for the one or more electronic components;

connecting a first one of the base and cover portions to a power supply;

connecting a second one of the base and cover portions to the power supply through an electrical contact with the first one of the base and cover portions;

electrically supporting, with the second one of the base and cover portions, one or more of the one or more electronic components that store one or more private keys; and

disconnecting the power supply from one or more of the one or more electronic components to erase the one or more private keys if the current location of the authentication device does not match the initial location of the authentication device.

22. An article, comprising:

one or more computer-readable signal-bearing media;

means in the one or more media for receiving a request from a second computing device to authenticate a first computing device for a data transfer from the second computing device to the first computing device;

means in the one or more media for determining a current location of an authentication device, in communication with the first computing device, in response to the request from the second computing device; and

means in the one or more media for authenticating the first computing device if the current location of the authentication device matches an initial location of the authentication device.

* * * * *